AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT APPLICATIONS

I, Jonathan A. Duquette, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following:

a. The premises known as 25 Elmwood Street, Portland, Maine (hereafter "Premises"), further described in Attachment A1, for the things described in Attachment B1; and

b. The person of Andrew Hazelton and any personal effects in his actual possession, further described in Attachment A2, for the things described in Attachment B2.

2. I am a Task Force Officer with the Federal Bureau of Investigation (FBI). I have been in this position since June 2015, and I have been a Task Force Officer in FBI's Boston Division since January 2018. I am also a Border Patrol Agent with the U.S. Border Patrol and have been in this position since December 2009. In my career, I have utilized various investigative tools and techniques, to include the use of search warrants.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for federal criminal offenses. I also am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants. Based on my training and experience and the facts as set forth in this affidavit, I submit that probable cause exists to believe that Andrew Hazelton attempted to sexually exploit a minor, in violation of 18 U.S.C. § 2251(a) and (e); and attempted to possess

child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2). I submit that there is also probable cause to search the locations described in Attachments A1 and A2 for evidence of these crimes, further described in Attachments B1 and B2.

APPLICABLE STATUTES

5. Based on my conversations with personnel from the U.S. Attorney's Office for the District of Maine, I am aware that Title 18, United States Code, Section 2251(a) provides that any person who "persuades, induces, entices, or coerces any minor to engage in … any sexually explicit conduct for the purpose of producing any visual depiction of such conduct" is guilty of an offense. Subsection (e) of the same statute also prohibits attempts to violate the statute. "Sexually explicit conduct" includes the lascivious exhibition of the anus, genitals, or pubic area of any person.

6. I am also aware that Title 18, United States Code, Section 2252A(a)(5)(B) provides that any person who knowingly possesses any "material that contains an image of child pornography that has been … transported using any means or facility of interstate or foreign commerce ort in or affecting interstate or foreign commerce by any means, including by computer," is guilty of an offense. Subsection (b)(2) of the same statute also prohibits attempts to violate the statute.

PROBABLE CAUSE

Penobscot County Sheriff's Office Investigation

7. On October 2, 2019, the Penobscot County Sheriff's Office received a complaint from A.L., a resident of Bradley, Maine and the mother of a 10-year-old girl, to whom I will refer as Victim 1 in this affidavit. Deputy Peter Stone met A.L. at her residence in Bradley. A.L.,

who was visually upset, told Stone that Victim 1 had been on Instagram the previous night and had sent inappropriate pictures to a 24-year-old man.

8. A.L. told Stone that she had been in Victim 1's room earlier in the day and noticed that Victim 1's phone was going off. She picked up the phone to see what was happening with it, and found that the phone's password had been changed. With the help of her son, A.L. was able to unlock the phone. She discovered that Victim 1 had sent several pictures, including one of her without a shirt and others of the front and back of her underwear. She also noted that in reply, a male had said he wanted to have sex with Victim 1. A.L. said she had reset Victim 1's phone before Stone arrived.

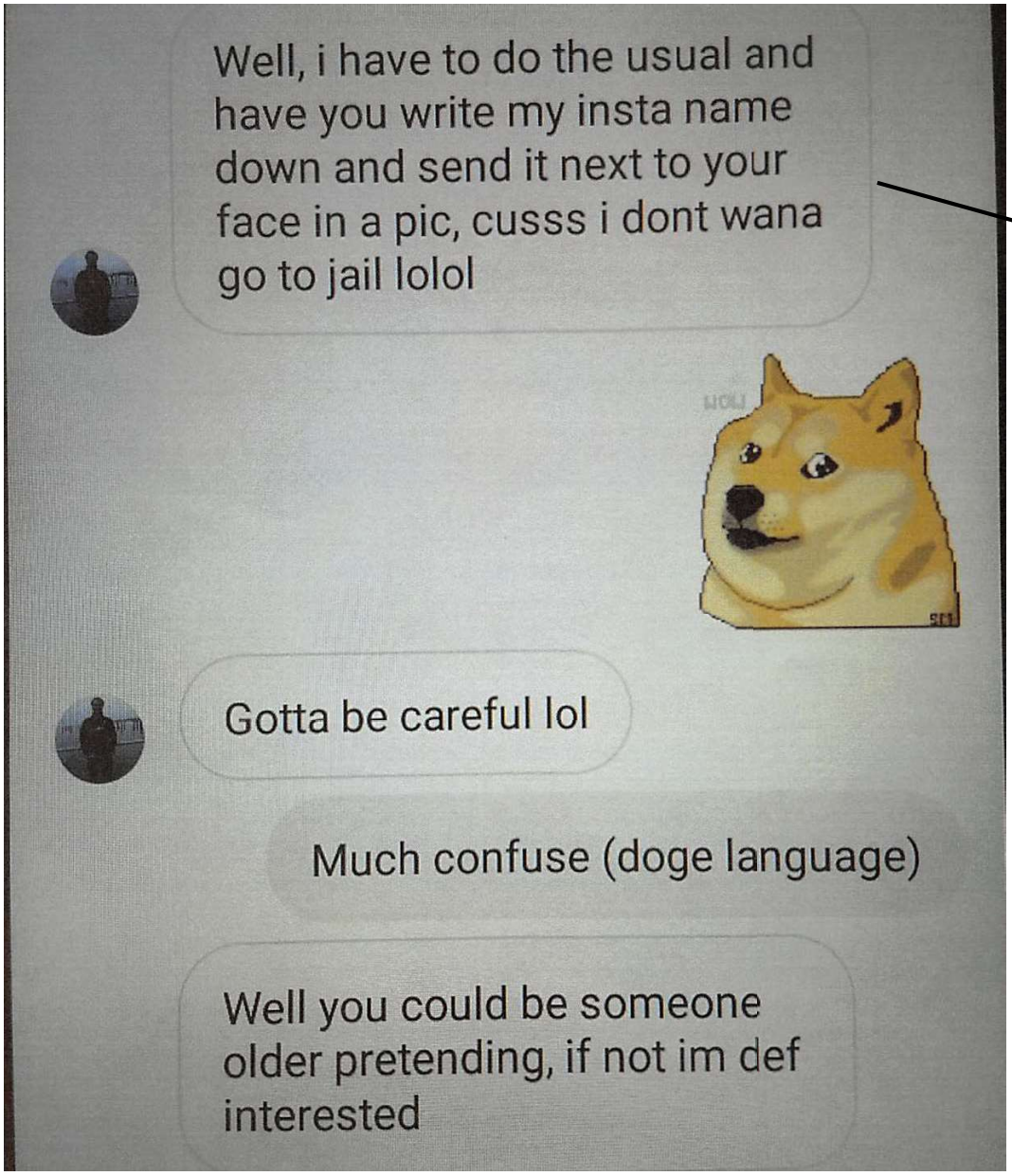
9. Detective William Flagg of the Penobscot County Sheriff's Office also responded to A.L.'s residence and took possession of Victim 1's phone and laptop with A.L.'s consent. Flagg turned over the devices to Detective Sergeant Noel Santiago, who was able to restore Victim 1's phone. Santiago was able to retrieve the online chat that Victim 1 had via Instagram with someone using the username hazelman93.[1] The user also identified himself as "Andrew."

10. The following are screenshots Santiago took of the Instagram chat between Victim 1 and hazelman93:

(The rest of this page was left blank intentionally)

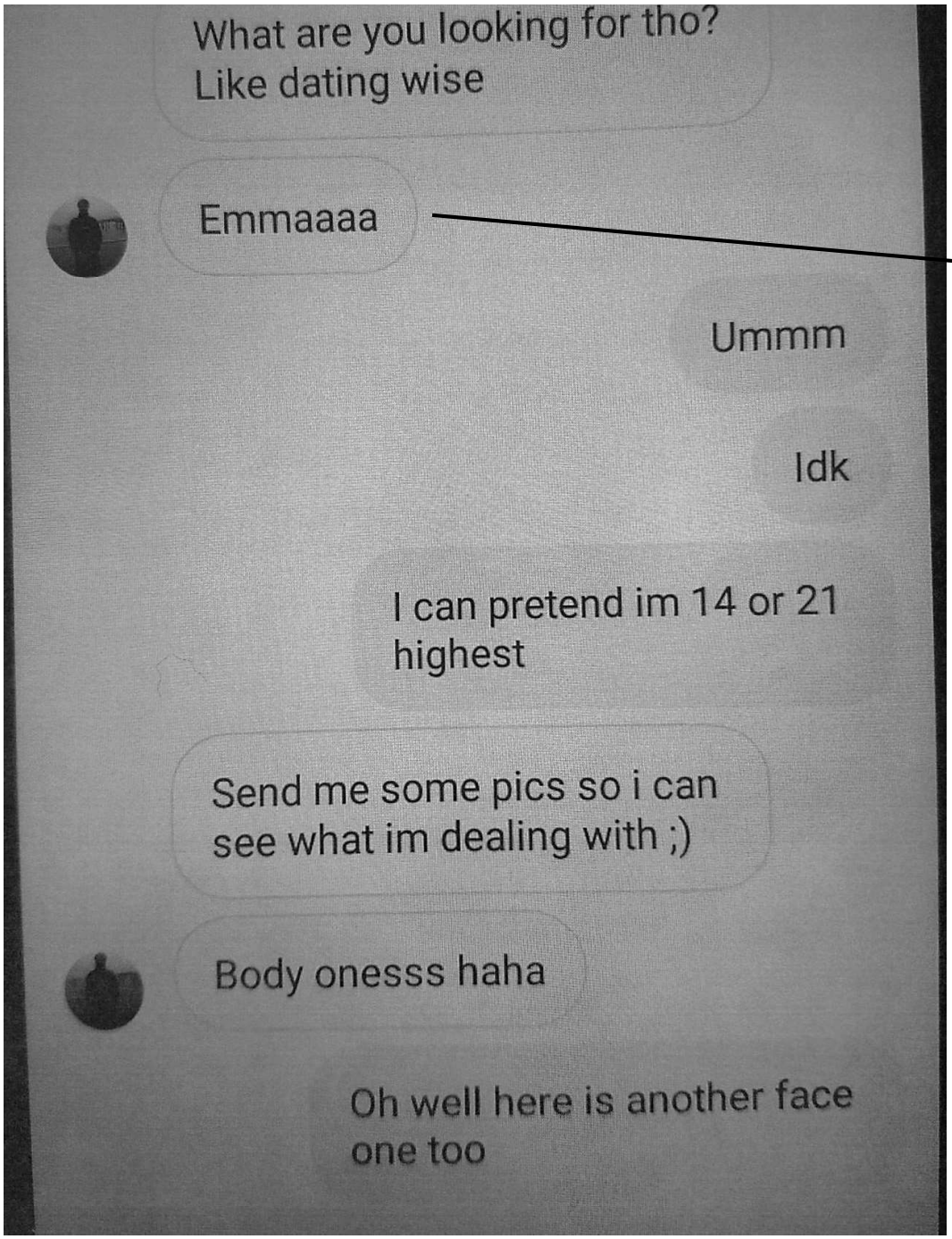
[1] Instagram is a free-access social networking service owned by Facebook that is accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, through which users can share messages, multimedia, and other information with other Instagram users and the general public. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups


hazelman93
Andrew
Tue 4:38 PM
Hey you ;)
Hi
So how old are you lol
10. BIGGG OOOOOOOF
And you legit like someone as old as me?
Yea



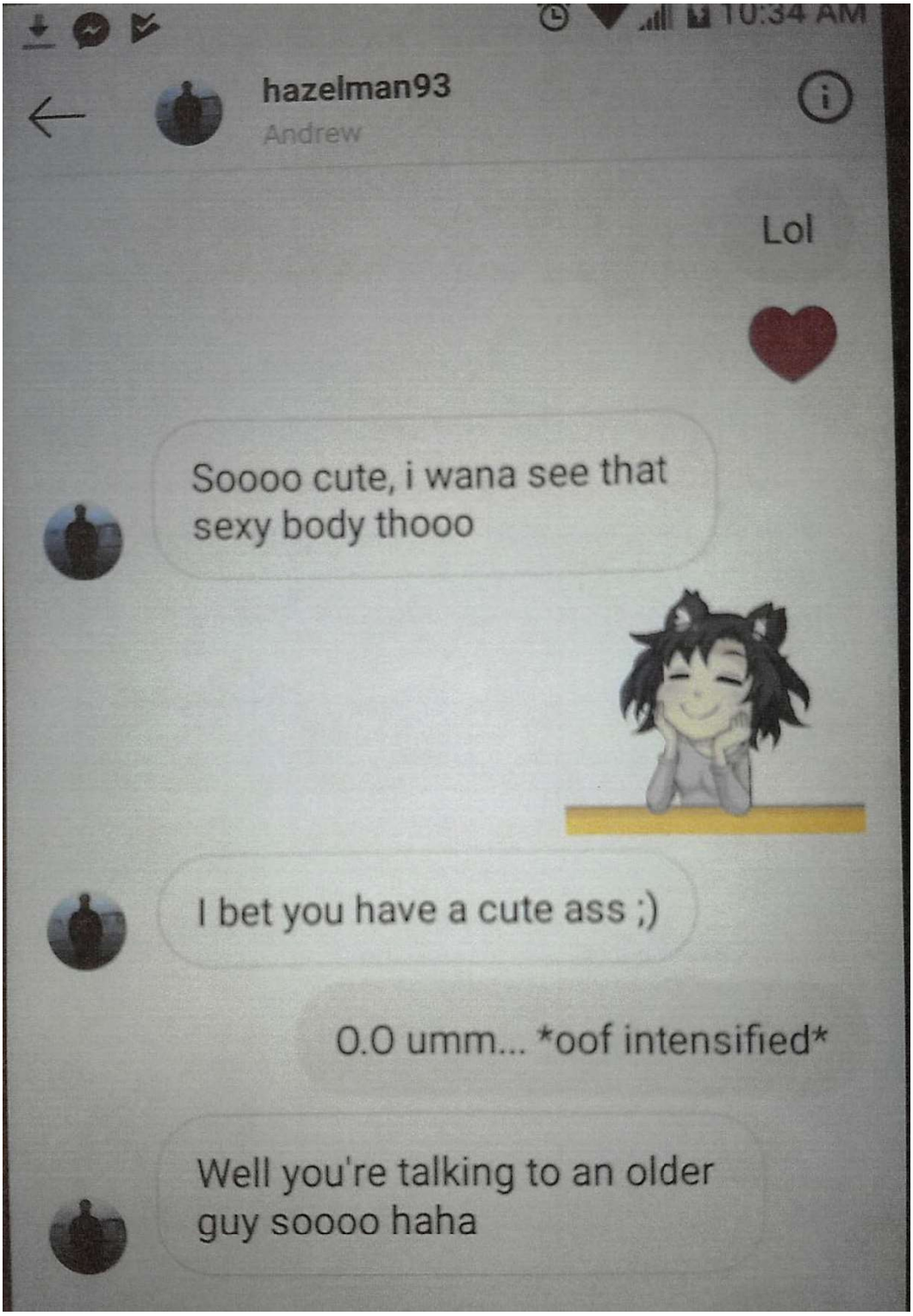
(See FN 2)

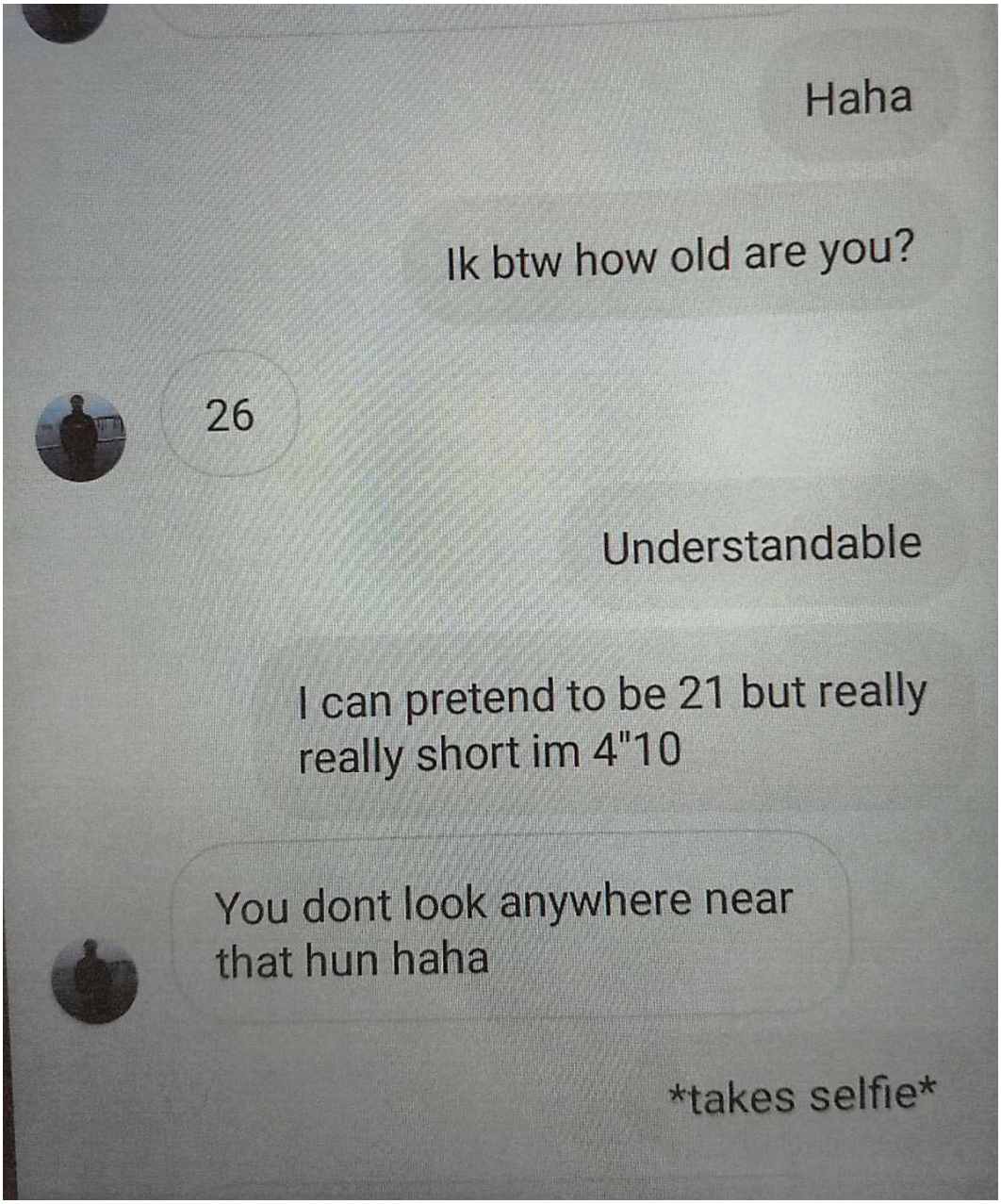
[2] Based on my training and experience, as well as information provided by other investigators, I know it is common for individuals engaged in sexually explicit online conversations with other individuals who claim to be minors to request that the purported minor provide some proof that they are an actual minor and not an undercover law enforcement officer. This is often accomplished by having the minor take a photograph with something showing that the photograph is being taken contemporaneously with the online chat.

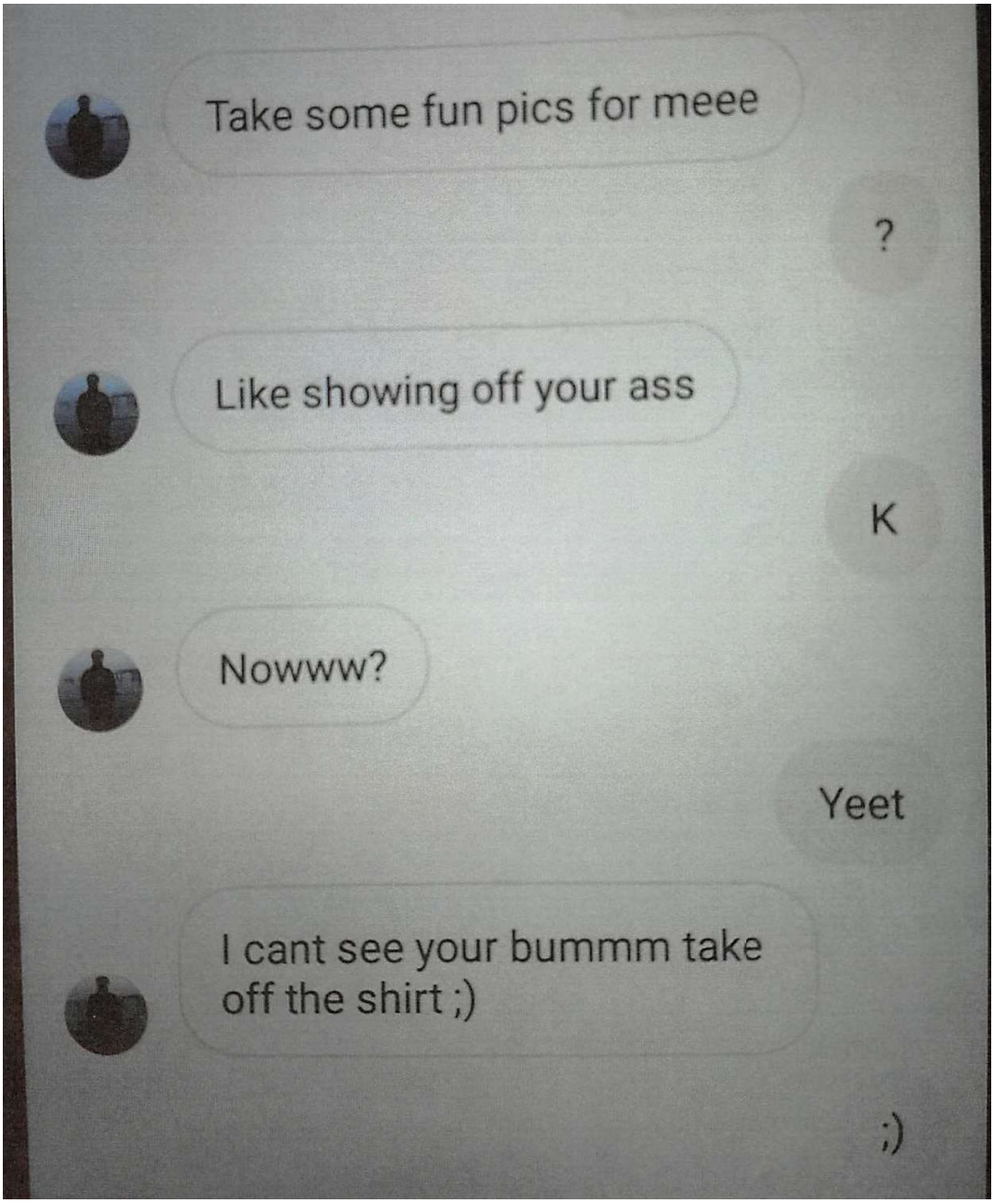


(See FN 3)

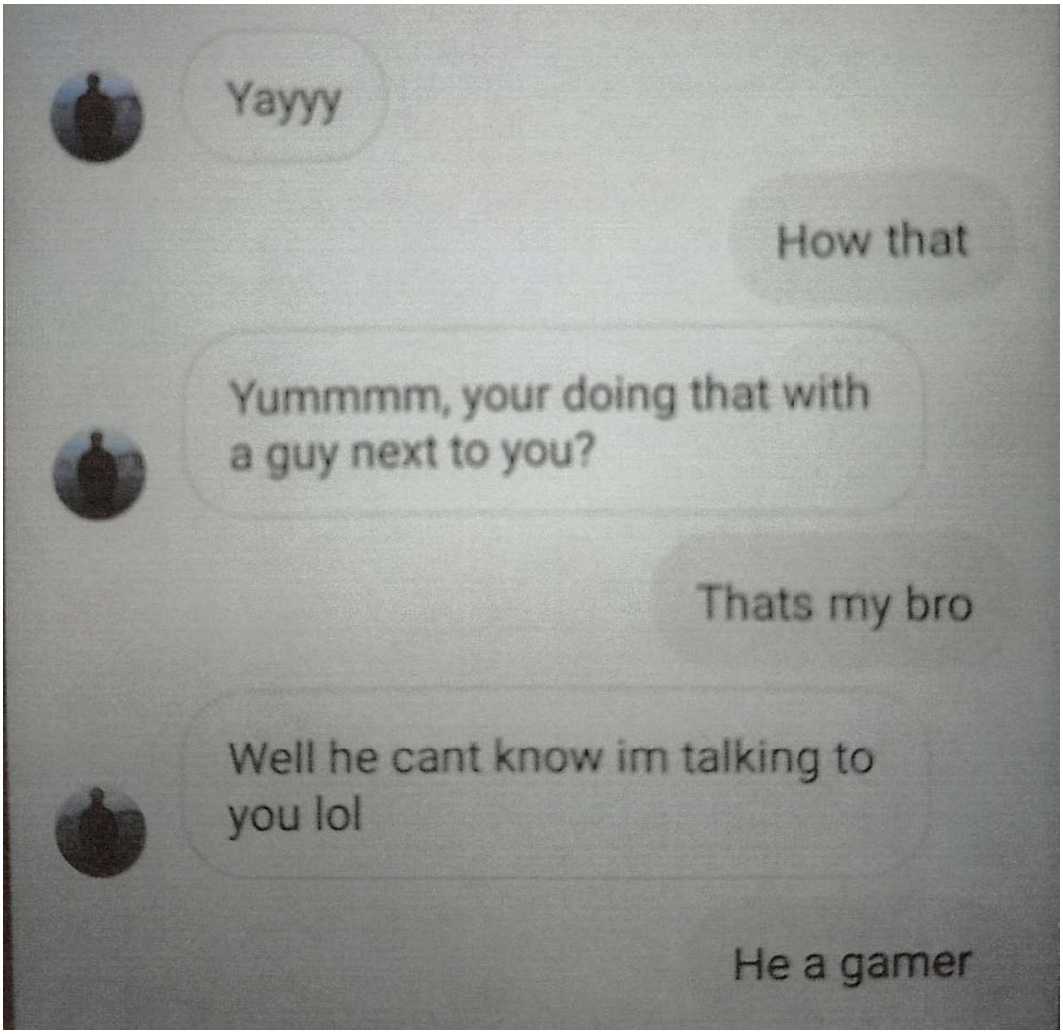
[3] "Emma_xgacha" was the username of the Instagram account Victim 1 was using at the time of her chat with hazelman93. Emma is not Victim 1's actual first name.

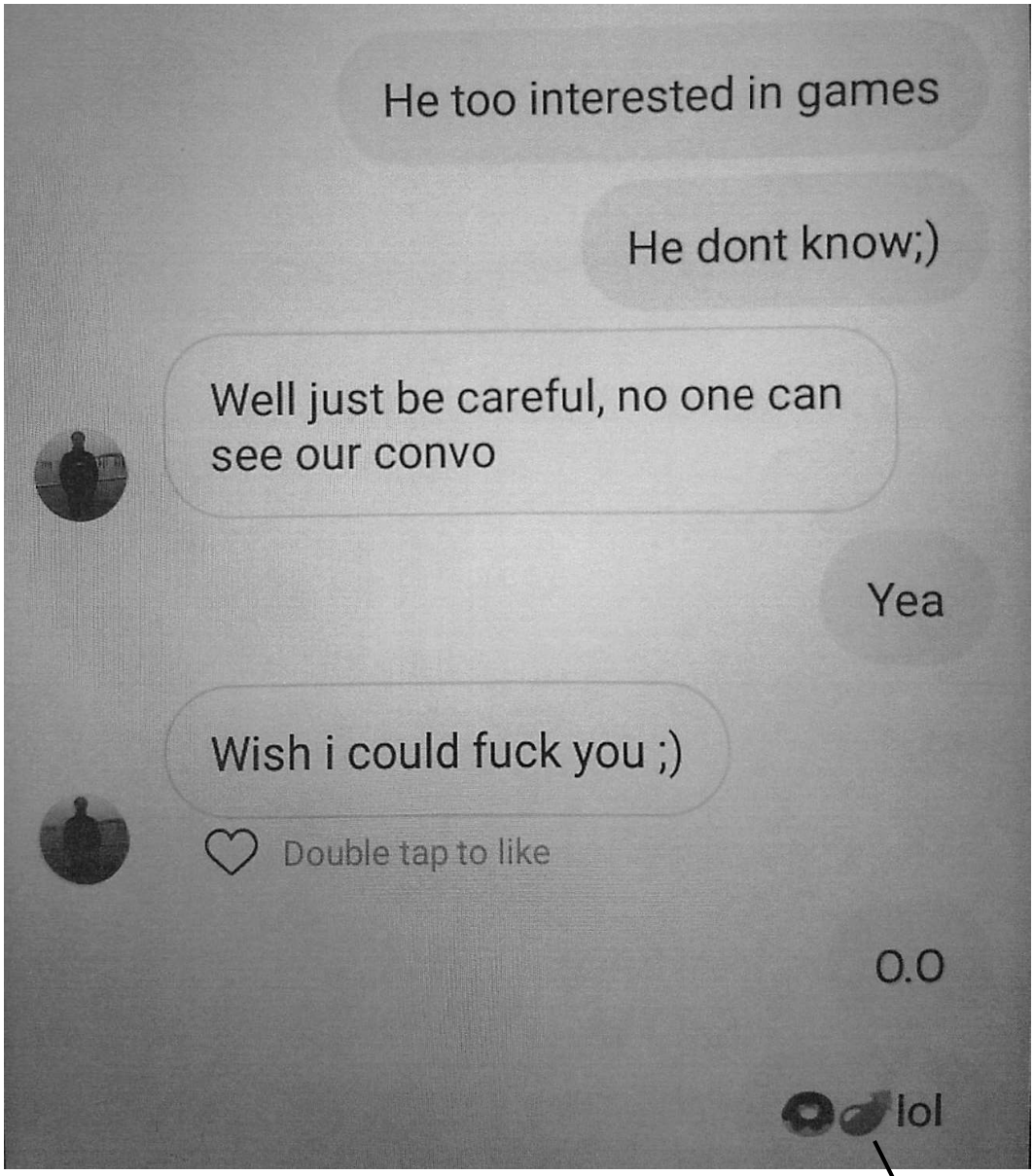

10:34 AM
hazelman93
Andrew
Lol
Soooo cute, i wana see that sexy body thooo
I bet you have a cute ass ;)
0.0 umm... *oof intensified*
Well you're talking to an older guy soooo haha


Haha
Ik btw how old are you?
26
Understandable
I can pretend to be 21 but really really short im 4"10
You dont look anywhere near that hun haha
takes selfie


Take some fun pics for meee
?
Like showing off your ass
K
Nowww?
Yeet
I cant see your bummm take off the shirt ;)
;)

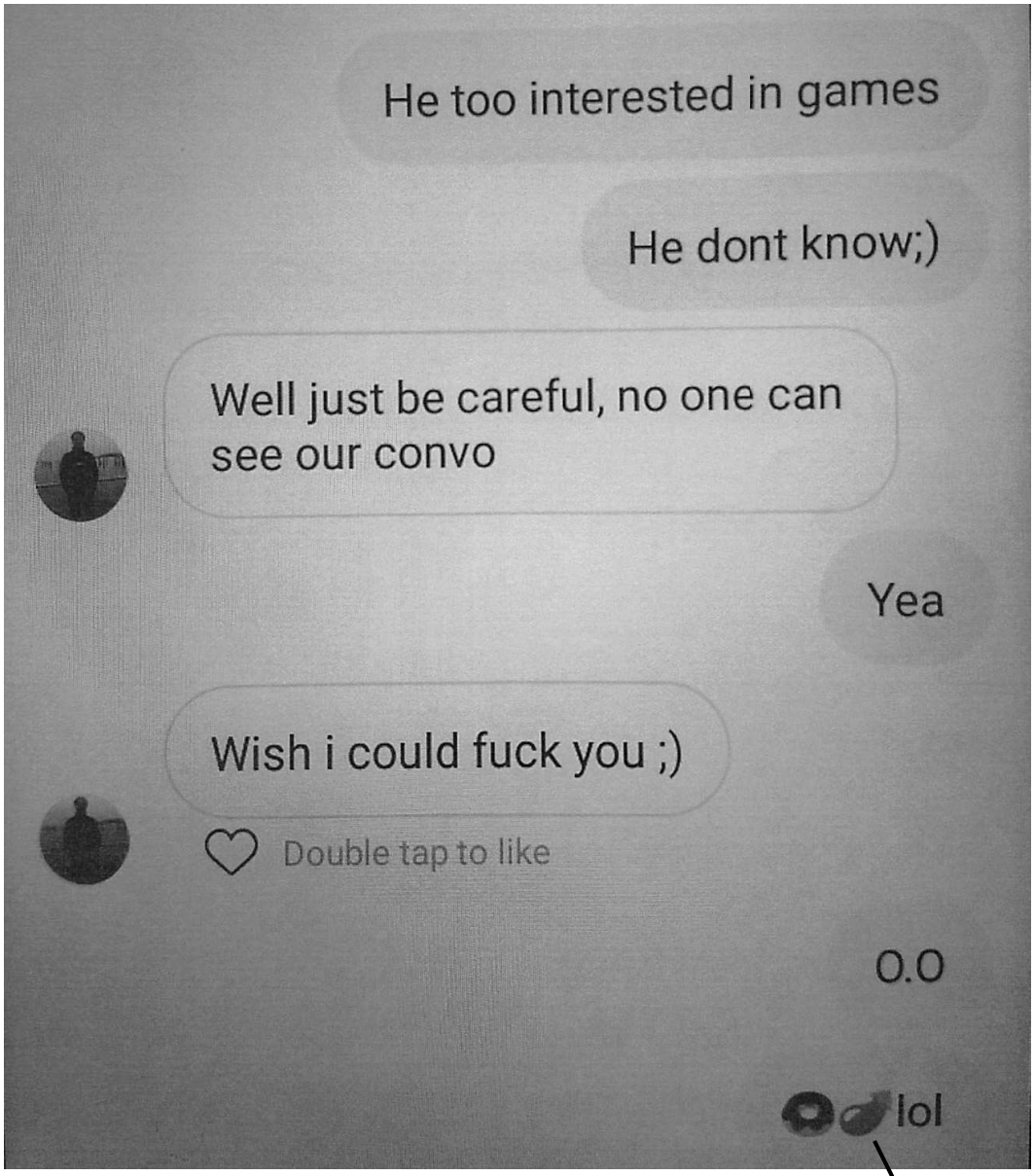

I wana see your panties ;)
Im thiccc
Im in love haha, take the shirt off? ;?
;)*
Im cold but i can do pic in the shirt;)
Just for a seconddd i wana see all of you ;)
Oh ok;)


Yayyy
How that
Yummmm, your doing that with a guy next to you?
Thats my bro
Well he cant know im talking to you lol
He a gamer



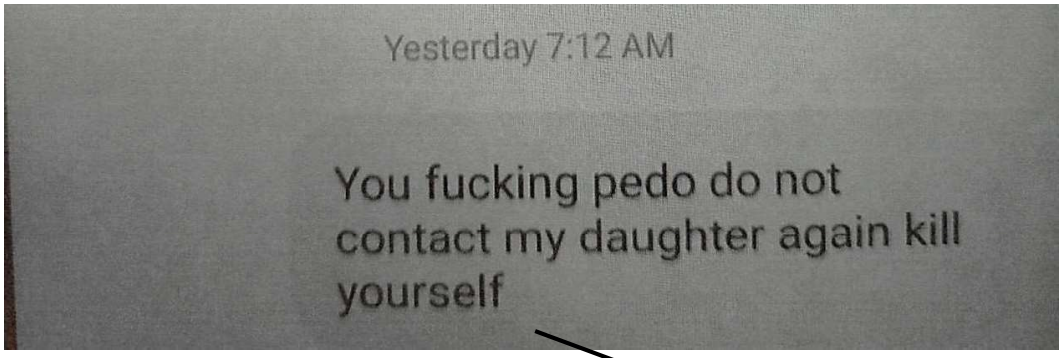
(See FN 4)

[4] Based on my training and experience, I know that these emojis are commonly used to signify sexual intercourse.



(See FN 4)

[4] Based on my training and experience, I know that these emojis are commonly used to signify sexual intercourse.



(See FN 5)

9. Santiago located the profile for hazelman93 on Instagram and noted that the profile was open for the public to view. He was able to open hazelman93's photos and observed that hazelman93 was a male, and in one of the photos there was a red-colored vehicle with a Toyota emblem on the front. There was a second photo of a vehicle inspection report from Joe's Citgo in Westford, Massachusetts. The vehicle was a 2002 Toyota Camry with Massachusetts registration plate number 54NX29 and Vehicle Identification Number 4T1BE32K32U092710.

10. Santiago requested a registration check on plate number 54NX29 from dispatch and learned that the vehicle was a red 2002 Toyota Camry registered to Susan G. Hazelton, with an address in Westford, Massachusetts.

11. Noting that hazelman93 had identified himself as "Andrew," Santiago looked up Andrew Hazelton on Facebook and located a profile for a male with that name. The profile stated that Hazelton had attended UMass Lowell, lived in Portland, Maine and was from Westford, Massachusetts. Like the Instagram profile, the Facebook page for Andrew Hazelton was open to the public and Santiago was able to look at the photos associated with the account. One of the

[5] This final message was written by A.L. and sent to hazelman93.

photos was the Instagram profile photo from hazelman93. There were also two other photos of the same-colored vehicle that was in hazelman93's Instagram photos.

12. Santiago asked dispatch to run a query on an Andrew Hazelton in Massachusetts. Dispatch located an Andrew Hazelton with a date of birth in February 1993 and the same address in Westford, Massachusetts as Susan Hazelton.

13. Santiago also searched open-source databases for Andrew Hazelton, and learned that as of May 31, 2019, Hazelton was living at 841 Broadway in South Portland, Maine.

Identification of the Premises as Andrew Hazelton's Residence

14. In April of this year, I learned of A.L.'s October 2019 complaint and Detective Santiago's subsequent investigation. Through open-source information as well as surveillance, I learned that the Andrew Hazelton identified by Santiago as the user of the Instagram username hazelman93 currently resides at the Premises.

15. Information provided by Central Maine Power indicates that electrical service to the Premises is in the name of Loan Nguyen. The public website for the Portland, Maine tax assessor likewise shows that the owner of the Premises is "Nguyen Loan T." The assessor's website describes the residence as a three-bedroom residence.

16. Based on a review of vehicle registration records, information from the U.S. Postal Service and other means, I have learned that Andrew Hazelton resides at the Premises with a roommate.

Means and Facilities of Interstate Commerce

17. Based on my conversations with personnel from the U.S. Attorney's Office, I am aware that courts have concluded that the internet is a means and facility of interstate commerce. Therefore, when Hazelton solicited Victim 1, he was attempting to persuade her to send him

sexually explicit images using a means and facility of interstate commerce. Likewise, he similarly attempted to possess images of child pornography that if sent by Victim 1, would have been transported using a means and facility of interstate commerce. Finally, in his Instagram chats with Victim 1, Hazelton was himself using a means and facility of interstate commerce to attempt to commit violations of 18 U.S.C. §§ 2251(a) and 2252A(a)(5)(B).

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, PROCURE OR POSSESS CHILD PORNOGRAPHY

18. As a result of my consultations with other law enforcement officers who have considerable experience investigating the sexual exploitation of children, I have learned about individuals engaged in child exploitation activities and about the computer technology available to, and utilized by, those individuals. I know there are certain characteristics common to individuals I have learned that individuals engaged in the production, procurement, trade, and/or transmission of child pornography through a computer or other interstate conveyance:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if a target such as Andrew Hazelton uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the Premises, as set forth in Attachment A1, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

19. Based on the foregoing, I believe that the investigation thus far shows that Andrew Hazelton, using the Instagram username hazelman93, likely displays characteristics common to individuals who engage in the production, procurement, trade, and/or transmission of child pornography. In particular, Hazelton enticed Victim 1, whom he knew to be a 10-year-old girl, to send him sexually suggestive photographs and later in the same chat told Victim 1, "Wish I could fuck you." Hazelton also stated during the chat that if Victim 1 was really 10 years old and not an older person pretending to be younger, he would definitely be interested in her. I submit that probable cause exists to believe that absent intervention by Victim 1's mother, Hazelton would have escalated his behavior and requested more sexually explicit images from Victim 1. I further submit that Hazelton's interactions with Victim 1 constituted a substantial step toward persuading her to create and send images constituting child pornography.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in Attachments B1 and B2, this application seeks permission to search for records that might be found on the Premises or in the possession of Andrew Hazelton, in whatever form they are found. One form in which the records might be

found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Probable cause.* I submit that if a computer or storage medium is found on the Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files.

Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. *Forensic evidence.* As further described in Attachments B1 and B2, these applications seek permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Premises or on the person of Andrew Hazelton because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used.

c. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was

created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such devices were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

g. I know that when an individual uses a digital device to attempt to sexually exploit a minor, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires

considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

25. Upon securing the Premises, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B1 and transport these items to an appropriate law enforcement laboratory or similar facility for review. Similarly, law enforcement personnel will seize any digital devices found in Hazelton's actual possession. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the Premises or where Hazelton is found. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachments B1 and B2.

26. Because multiple people share the Premises as a residence, it is possible that the Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

BIOMETRIC ACCESS TO DEVICES

27. The warrants for which I am applying permit law enforcement to compel Andrew Hazelton to unlock any electronic devices found at the Premises or on his person requiring biometric access subject to seizure pursuant to the warrants. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, based on Andrew Hazelton's use of Instagram, I have reason to believe that one or more digital devices will be found during the execution of the two search warrants for which I am applying. The passcode or password that would unlock the devices subject to search under these warrants currently are not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that

biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to these warrants and may be unlocked using one of the aforementioned biometric features, these warrants permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Andrew Hazelton to the fingerprint scanner of the devices found at the Premises or on his person; (2) hold the devices found at the Premises or on Hazelton's person in front of Hazelton's face and activate the facial recognition feature; and/or (3) hold the devices found at the Premises or on Hazelton's person in front of Hazelton's face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by these warrants. The proposed warrants do not authorize law enforcement to compel that Hazelton state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrants do not authorize law enforcement to compel Hazelton to identify the specific biometric

characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

28. Based on the forgoing, I submit that probable cause exists to believe that violations of 18 U.S.C. § 2251(a) and (e); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), have occurred, and that the evidence and instrumentalities of these offenses, more fully described in Attachments B1 and B2, are located at the locations described in Attachments A1 and A2. I respectfully request that the Court issue search warrants for the locations described in Attachment A1 and A2, authorizing the seizure and search of the items described in Attachments B1 and B2.

Dated at Portland, Maine this 28th day of April, 2021.

Jonathan A. Duquette
Task Force Officer
Federal Bureau of Investigation

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedure

Date: Apr 28 2021

City and state: Portland, ME

Judge's signature

John H. Rich III, U.S. Magistrate Judge

Printed name and title